

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-155834

(P2000-155834A)

(43) 公開日 平成12年6月6日(2000.6.6)

(51) Int.Cl.	識別記号	F I	テーマコード(参考)
G 0 6 T 1/00		G 0 6 F 15/66	B 5 B 0 5 7
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 D 5 C 0 7 6
		5/00	5 J 1 0 4
H 0 4 L 12/28		H 0 4 N 1/387	5 K 0 3 0
12/54		H 0 4 L 11/00	3 1 0 Z 5 K 0 3 3

審査請求 未請求 請求項の数26 O L (全 10 頁) 最終頁に続く

(21) 出願番号 特願平10-330837

(22) 出願日 平成10年11月20日(1998.11.20)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 吉田 淳

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(72) 発明者 岩村 恵市

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(74) 代理人 100090273

弁理士 國分 孝悦

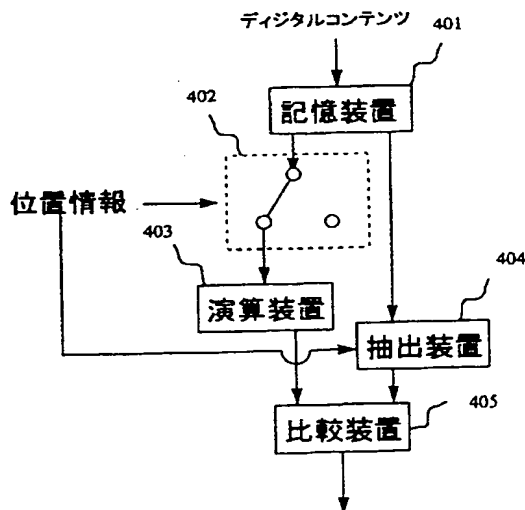
最終頁に続く

(54) 【発明の名称】 不正検知装置、方法、電子透かし埋め込み装置、方法及びコンピュータ読み取り可能な記憶媒体

(57) 【要約】

【課題】 デジタルコンテンツに埋め込まれている電子透かしに対して改竄等の不正がなされたことを検知する。

【解決手段】 記憶装置401からハッシュ値が電子透かしとして埋め込まれているデジタルコンテンツが読み出され、このデジタルコンテンツから、スイッチ401により、位置情報に基づいてハッシュ値の演算に用いたハッシュ対象部分集合を抽出して演算装置403に投入し、ハッシュ値を求める。一方、抽出装置404は、上記デジタルコンテンツから位置情報に基づいてハッシュ値を抽出する。上記演算装置403で求めたハッシュ値と、上記抽出されたハッシュ値とが比較装置405で比較され、一致していればデジタルコンテンツが正当であり、一致していなければ不正であるとする。



BEST AVAILABLE COPY

## 【特許請求の範囲】

【請求項1】 入力されるデジタルコンテンツを構成しているデータ値の部分集合の複数個を選択する選択手段と、

上記選択された複数の部分集合のうち、所定の1つ又は複数の部分集合に含まれるデータ値を用いて各部分集合毎に所定の演算を行う演算手段と、

上記選択された複数の部分集合のうち、他の所定の1つ又は複数の部分集合から電子透かしとして埋め込まれている情報をそれぞれ抽出する透かし抽出手段と、

上記演算手段により求めた値とこの値を求めた部分集合とは異なる部分集合から抽出された上記情報とを比較する比較手段とを設けたことを特徴とする不正検知装置。

【請求項2】 上記演算手段は、上記選択された部分集合に含まれるデータ値のハッシュ値を求めることを特徴とする請求項1記載の不正検知装置。

【請求項3】 上記選択された複数の部分集合のデジタルコンテンツ上の位置が連続していることを特徴とする請求項1記載の不正検知装置。

【請求項4】 上記デジタルコンテンツに含まれる全てのデータ値が、上記選択された部分集合に含まれることを特徴とする請求項1記載の不正検知装置。

【請求項5】 上記デジタルコンテンツに含まれる全てのデータ値が、上記選択された部分集合に多重に含まれることを特徴とする請求項1記載の不正検知装置。

【請求項6】 上記選択された複数の部分集合を構成する要素のデジタルコンテンツ上の位置が、デジタルコンテンツ全体に均一に分布していることを特徴とする請求項1記載の不正検知装置。

【請求項7】 上記デジタルコンテンツがデジタル画像であり、上記選択された複数の部分集合を構成する要素のデジタルコンテンツ上の位置が、上記デジタル画像上で千鳥状に分布していることを特徴とする請求項6記載の不正検知装置。

【請求項8】 上記デジタルコンテンツがデジタル画像であり、上記選択された複数の部分集合を構成する要素のデジタルコンテンツ上の位置が、上記デジタル画像上で縞状に分布していることを特徴とする請求項6記載の不正検知装置。

【請求項9】 上記デジタルコンテンツがデジタル画像であり、上記選択された複数の部分集合を構成する要素のデジタルコンテンツ上の位置が、上記デジタル画像上で格子状に分布していることを特徴とする請求項6記載の不正検知装置。

【請求項10】 上記選択された部分集合が、デジタルコンテンツ上のオブジェクトであることを特徴とする請求項1記載の不正検知装置。

【請求項11】 上記デジタルコンテンツ上の所定の位置に電子透かしとして埋め込まれている埋め込み位置

情報を抽出する位置抽出手段を設け、上記抽出した埋め込み位置情報に示されるデジタルコンテンツ上の部分集合より、上記選択手段が複数の部分集合を選択することを特徴とする請求項1記載の不正検知装置。

【請求項12】 デジタルコンテンツを構成しているデータ値の部分集合の複数個を選択する選択手段と、上記選択された複数の部分集合のうち、所定の1つ又は複数の部分集合に含まれるデータ値を用いて各部分集合毎に所定の演算を行う演算手段と、

10 上記選択された部分集合のうち、他の所定の1つ又は複数の部分集合に、他の部分集合から上記演算手段が演算して求めた値を電子透かしとして埋め込む埋め込み手段とを設けたことを特徴とする電子透かし埋め込み装置。

【請求項13】 上記演算手段は、上記選択された部分集合のデータ値のハッシュ値を求めることを特徴とする請求項12記載の電子透かし埋め込み装置。

【請求項14】 上記選択された部分集合のデジタルコンテンツ上の位置が連続していることを特徴とする請求項12記載の電子透かし埋め込み装置。

20 【請求項15】 上記デジタルコンテンツに含まれる全てのデータ値が、上記選択された部分集合に含まれることを特徴とする請求項12記載の電子透かし埋め込み装置。

【請求項16】 上記デジタルコンテンツに含まれる全てのデータ値が、上記選択された部分集合に多重に含まれることを特徴とする請求項12記載の電子透かし埋め込み装置。

【請求項17】 上記選択された複数の部分集合を構成する要素のデジタルコンテンツ上の位置が、デジタルコンテンツ全体に均一に分布していることを特徴とする請求項12記載の電子透かし埋め込み装置。

30 【請求項18】 上記デジタルコンテンツがデジタル画像であり、上記選択された複数の部分集合を構成する要素のデジタルコンテンツ上の位置が、上記デジタル画像上で千鳥状に分布していることを特徴とする請求項17記載の電子透かし埋め込み装置。

【請求項19】 上記デジタルコンテンツがデジタル画像であり、上記選択された複数の部分集合を構成する要素のデジタルコンテンツ上の位置が、上記デジタル画像上で縞状に分布していることを特徴とする請求項17記載の電子透かし埋め込み装置。

40 【請求項20】 上記デジタルコンテンツがデジタル画像であり、上記選択された複数の部分集合を構成する要素のデジタルコンテンツ上の位置が、上記デジタル画像上で格子状に分布していることを特徴とする請求項17記載の電子透かし埋め込み装置。

【請求項21】 上記選択された部分集合が、デジタルコンテンツ上のオブジェクトであることを特徴とする請求項12記載の電子透かし埋め込み装置。

【請求項22】 上記デジタルコンテンツ上の所定の

位置に、上記選択された複数の部分集合の位置を示す位置情報を埋め込む位置情報埋め込みを手段を設けたことを特徴とする請求項1記載の電子透かし埋め込み装置。

【請求項23】 入力されるデジタルコンテンツを構成しているデータ値の部分集合の複数個を選択する手順と、

上記選択された複数の部分集合のうち、所定の1つ又は複数の部分集合に含まれるデータ値を用いて各部分集合毎にハッシュ値を演算する手順と、

上記選択された複数の部分集合のうち、他の所定の1つ又は複数の部分集合からハッシュ値として埋め込まれている電子透かし情報をそれぞれ抽出する手順と、

上記演算手順により求めたハッシュ値とこのハッシュ値を求めた部分集合とは異なる部分集合から抽出された上記電子透かし情報とを比較する手順とを設けたことを特徴とする不正検知方法。

【請求項24】 デジタルコンテンツを構成しているデータ値の部分集合の複数個を選択する手順と、

上記選択された複数の部分集合のうち、所定の1つ又は複数の部分集合に含まれるデータ値を用いて各部分集合毎にハッシュ値を演算する手順と、

上記選択された部分集合のうち、他の所定の1つ又は複数の部分集合に、他の部分集合から上記演算により求めたハッシュ値を電子透かしとして埋め込む手順とを設けたことを特徴とする電子透かし埋め込み方法。

【請求項25】 入力されるデジタルコンテンツを構成しているデータ値の部分集合の複数個を選択する処理と、

上記選択された複数の部分集合のうち、所定の1つ又は複数の部分集合に含まれるデータ値を用いて各部分集合毎にハッシュ値を演算する処理と、

上記選択された複数の部分集合のうち、他の所定の1つ又は複数の部分集合からハッシュ値として埋め込まれている電子透かし情報をそれぞれ抽出する処理と、

上記演算により求めたハッシュ値とこのハッシュ値を求めた部分集合とは異なる部分集合から抽出された上記電子透かし情報とを比較する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項26】 デジタルコンテンツを構成しているデータ値の部分集合の複数個を選択する処理と、

上記選択された複数の部分集合のうち、所定の1つ又は複数の部分集合に含まれるデータ値を用いて各部分集合毎にハッシュ値を演算する処理と、

上記選択された部分集合のうち、他の所定の1つ又は複数の部分集合に、他の部分集合から上記演算により求めたハッシュ値を電子透かしとして埋め込む処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子透かしが埋め込まれたデジタルコンテンツに対する改竄等の不正を検知する不正検知装置、方法、電子透かしを埋め込む電子透かし埋め込み装置、方法及びそれらに用いられるコンピュータ読み取り可能な記憶媒体に関するものである。

【0002】

10 【従来の技術】デジタル情報には、従来のアナログ情報と比較し、コンピュータなどによって簡単に劣化すること無くコピー、改竄でき、通信回線を通じて転送することが容易であるという特徴がある。このような特徴により、デジタル情報は安易に不正コピーされ再配布される傾向にあった。

【0003】これを防ぐための方法の一つとして、電子透かしと呼ばれる手法がある。電子透かしとは、それを埋め込んであるデジタルコンテンツを通常に再生した場合には、人間には知覚できない形で情報を埋め込む手法である。尚、以下の説明において、デジタルコンテンツとは、動画像、静止画像、音声、コンピュータプログラム及びコンピュータデータ等を指すものとする。

20 【0004】電子透かしによる情報埋め込み方式の代表的なものとして、デジタル画像でいえば、画素の色相、明度等にあたる、デジタルコンテンツのデータ値に対し演算を施して電子透かしを埋め込む手法がある。この手法の代表的なものとして、デジタルコンテンツをブロックに分割し、ブロック毎に+1と-1の組み合わせである、予め決められた透かしパターンを足し込むというDigimarc社、米国特許5,636,292号の手法がある。

【0005】他の電子透かし埋め込み方法の代表的なものとしては、デジタルコンテンツに対し高速フーリエ変換、離散コサイン変換、ウェーブレット変換等の周波数変換を行い、周波数領域に透かし情報を加えた後、逆周波数変換を行うことにより埋め込みを行う手法が挙げられる。

30 【0006】高速フーリエ変換による手法では、入力コンテンツは、PN系列を加えられて拡散された後、ブロックに分割される。そして、ブロック毎にフーリエ変換が施され、1ブロックに1ビットの透かし情報が埋め込まれる。透かし情報が埋め込まれたブロックは逆フーリエ変換が施され、再び最初と同じPN系列が加えられて電子透かしが埋め込まれたコンテンツが得られる。この手法は、「大西、岡、松井、"PN系列による画像への透かし署名法"1997年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26B」に詳しく、

40 【0007】離散コサイン変換による手法は、ブロックに分割し、ブロック毎に離散コサイン変換をする。1ブ

ロックに1ビットの情報を埋め込んだ後、逆変換をして電子透かし埋め込み済みコンテンツを生成する。この手法は、「中村、小川、高嶋」デジタル画像の著作権保護のための周波数領域における電子透かし方式”1997年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26A」に詳しい。

【0008】ウェーブレット変換による手法は、入力コンテンツをブロック分割する必要のない手法であり、「石塚、酒井、櫻井、”ウェーブレット変換を用いた電子透かし技術の安全性と信頼性に関する実験的考察”1997年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26D」に詳しい。

【0009】上記のような方法により、デジタルコンテンツに電子透かしとして埋め込まれる情報の代表的なものとして、著作権情報とユーザ情報が挙げられる。著作権情報を埋め込むことにより、ユーザは、デジタルコンテンツに著作権が設定されていることや、著作者は誰であるか等を知ることができる。しかし、実際に著作権が保護されるか否かはユーザのモラルにかかっていた。また、ユーザ情報を埋め込むことにより、不正に再配布されたデジタルコンテンツより、再配布を行ったユーザを検知することができる。しかし、この場合もユーザに対して警告を発する程度の効果しか望めない。

【0010】今後、インターネット等のインフラがさらに整い、ネットワーク社会が進展するに連れて、デジタルコンテンツがネットワーク上で配信される機会が飛躍的に増加することが予測される。それに伴いより深刻になってくるのが著作権保護に関する問題であり、この問題の解決のために、場合によっては著作権の設定されていないデジタルコンテンツも含む全てのデジタルコンテンツに電子透かしが埋め込まれることが一般的になると考えられる。

【0011】

【発明が解決しようとする課題】しかしながら、上記のように著作権保護のために、従来の方式で電子透かしを埋め込んだ場合においても、著作権が守られるか否かはユーザの意識にかかり、物理的に著作権の保護を行うことはできないという問題があった。

【0012】本発明は、上記の問題を解決するために成されたもので、デジタルコンテンツに対する不正を検知すること、及びデジタルコンテンツに不正の行われにくい電子透かしを埋め込むことができるようにすることを目的としている。

【0013】

【課題を解決するための手段】上記の目的を達成するために、本発明による不正検知装置においては、入力されるデジタルコンテンツを構成しているデータ値の部分集合の複数個を選択する選択手段と、上記選択された複数の部分集合のうち、所定の1つ又は複数の部分集合に含まれるデータ値を用いて各部分集合毎に所定の演算を

行う演算手段と、上記選択された複数の部分集合のうち、他の所定の1つ又は複数の部分集合から電子透かしとして埋め込まれている情報をそれぞれ抽出する透かし抽出手段と、上記演算手段により求めた値とこの値を求めた部分集合とは異なる部分集合から抽出された上記情報とを比較する比較手段とを設けている。

【0014】また、本発明による電子透かし埋め込み装置においては、デジタルコンテンツを構成しているデータ値の部分集合の複数個を選択する選択手段と、上記選択された複数の部分集合のうち、所定の1つ又は複数の部分集合に含まれるデータ値を用いて各部分集合毎に所定の演算を行う演算手段と、上記選択された部分集合のうち、他の所定の1つ又は複数の部分集合に、他の部分集合から上記演算手段が演算して求めた値を電子透かしとして埋め込む埋め込み手段とを設けている。

【0015】また、本発明による不正検知方法においては、入力されるデジタルコンテンツを構成しているデータ値の部分集合の複数個を選択する手順と、上記選択された複数の部分集合のうち、所定の1つ又は複数の部分集合に含まれるデータ値を用いて各部分集合毎にハッシュ値を演算する手順と、上記選択された複数の部分集合のうち、他の所定の1つ又は複数の部分集合からハッシュ値として埋め込まれている電子透かし情報をそれぞれ抽出する手順と、上記演算により求めたハッシュ値とこのハッシュ値を求めた部分集合とは異なる部分集合から抽出された上記電子透かし情報とを比較する手順とを設けている。

【0016】また、本発明による電子透かし埋め込み方法においては、デジタルコンテンツを構成しているデータ値の部分集合の複数個を選択する手順と、上記選択された複数の部分集合のうち、所定の1つ又は複数の部分集合に含まれるデータ値を用いて各部分集合毎にハッシュ値を演算する手順と、上記選択された部分集合のうち、他の所定の1つ又は複数の部分集合に、他の部分集合から上記演算により求めたハッシュ値を電子透かしとして埋め込む手順とを設けている。

【0017】また、本発明による記憶媒体においては、入力されるデジタルコンテンツを構成しているデータ値の部分集合の複数個を選択する処理と、上記選択された複数の部分集合のうち、所定の1つ又は複数の部分集合に含まれるデータ値を用いて各部分集合毎にハッシュ値を演算する処理と、上記選択された複数の部分集合のうち、他の所定の1つ又は複数の部分集合からハッシュ値として埋め込まれている電子透かし情報をそれぞれ抽出する処理と、上記演算により求めたハッシュ値とこのハッシュ値を求めた部分集合とは異なる部分集合から抽出された上記電子透かし情報とを比較する処理とを実行するためのプログラムを記憶している。

【0018】さらに、本発明による他の記憶媒体においては、デジタルコンテンツを構成しているデータ値の

部分集合の複数個を選択する処理と、上記選択された複数の部分集合のうち、所定の1つ又は複数の部分集合に含まれるデータ値を用いて各部分集合毎にハッシュ値を演算する処理と、上記選択されたデータ値の部分集合のうち、他の所定の1つ又は複数の部分集合に、他の部分集合から上記演算により求めたハッシュ値を電子透かしとして埋め込む処理とを実行するためのプログラムを記憶している。

【0019】

【発明の実施の形態】以下、本発明の実施の形態を図面と共に説明する。図1は、一般的なネットワークの構成を示す図であり、本発明の使用環境の一例を示す。公衆ネットワーク101の代表的なものとしてはインターネットが挙げられる。公衆ネットワーク101には、デジタル画像に代表される様々なデジタルコンテンツを販売、配布する配布サーバ102、警察機関103、ユーザ104、ローカルエリアネットワーク（LAN）105等が接続されている。

【0020】配布サーバ102は、World Wide Webサーバ（Webサーバ）により構成されるのが一般的である。またLAN105は、ファイアウォール106により外部から遮断され、LAN105—公衆ネットワーク101間では、送信者、送信データの種類など、予め設定されたパラメータを持つ通信のみが許可されている。

【0021】また、LAN105内部には、プロキシサーバ107、パーソナルコンピュータ（PC）108、PC108に接続されたディスプレイ109、プリンタ110、また他のPC111、他のPC111に接続されたディスプレイ112、LAN105に直接接続されたプリンタ113等が存在する。プロキシサーバ107は、LAN101内部のPC108、111が、配布サーバ102等のWebサーバにアクセスする際の制御を行っており、両者の間で通信されるデータは全てプロキシサーバ107を通過する。

【0022】図2は、本実施の形態による著作権保護方式を搭載したプロキシサーバ107の一例を示す図である。本システムは、システム内の装置間でのデータ交換に使用されるバス201、不正検知装置202、不正検知装置202の検出結果に従って動作する演算処理装置203、I/Oポート204、それぞれの装置を制御するコントローラ205、システムに入力されたデジタルコンテンツを一時的に保存するメモリ206、LAN105等システム外部のネットワークと接続されている通信ポート207、I/Oポート204に接続された外部記憶装置208及びディスプレイ209よりなる。

【0023】不正検知装置202は、予め電子透かし埋め込み装置によってデジタルコンテンツに埋め込まれた電子透かし情報を検出して、このデジタルコンテンツに対して不正な処理が行われたことを検知する。上記

電子透かし埋め込み装置が、デジタルカメラ、スキャナ等の画像入力装置に搭載された場合、この画像入力装置で入力したデジタルコンテンツに対して、不正が行われたことが不正検知装置202で検知可能となる。

【0024】また、電子透かし埋め込み装置が搭載されたコンピュータ、アプリケーションソフトウェアで、デジタルコンテンツを作成することにより、作成されたデジタルコンテンツに対する不正を不正検知装置202により検知可能である。また、電子透かし埋め込み装置は、記憶装置、配布サーバ、ネットワーク機器等に搭載される場合などがある。

【0025】本システムにおいて、調査対象となるデジタルコンテンツは、通信ポート207によって、LAN105及び／又はLAN105と公衆ネットワーク101等を通じて読み込まれる。読み込まれたデジタルコンテンツは、メモリ206に一時的に保存される。メモリ206上のデジタルコンテンツは、不正検知装置202に入力され、正当であるか否かが判定される。不正検知装置202でデジタルコンテンツが正当であると判定された場合は、通信ポート207によりデジタルコンテンツの配信依頼を行ったエンティティに対し配信される。

【0026】また、不正検知装置202で、デジタルコンテンツが不正であると判定された場合は、演算処理装置203により以下のいずれか一つ又は複数の処理が行われる。

・演算処理装置203によって、デジタルコンテンツに対してフィルタリング、暗号化、スクランブル、ノイズを加える等の、可視／不可視の電子透かしを埋め込む演算処理を行った後、通信装置207によってデジタルコンテンツの配信依頼を行ったエンティティに出力する。

【0027】・演算処理装置203によって、デジタルコンテンツを入手した入手元の情報、及び／又は読み込みを行ったエンティティの情報、及び／又はデジタルコンテンツの名称等、デジタルコンテンツに関する情報をI/Oポート204に接続された外部記憶装置208及び／又は通信ポート207を経由して配布サーバ102、警察機関103等に存在するデータベースへ書き込む。

【0028】・コントローラ204による制御によって出力を中止する。

・演算処理装置203によって、警告メッセージが発生され、I/Oポート204に接続されているディスプレイ209等に警告が表示される。また、通信ポート207によりネットワークを通じ、デジタルコンテンツの入手元、第三者機関に対して警告が発せられるシステムも容易に構成できる。

【0029】次に、不正検知装置202で用いる不正検出方法について説明する。本実施の形態による方法はハ

ッシュ値を用いた手法であるので、まずハッシュ値について説明する。ハッシュ値 $h$ とは、ハッシュ関数 $f: x \rightarrow h$ により求められる長い入力列 $X$ の圧縮値である短い出力 $h$ である。また、一方向性関数であり、 $f(x') = f(x)$ を満たす異なる入力 $x, x'$ を求めるのは難しいという性質を持つ。ハッシュ関数の代表的なものとしてMD5 (Message Digest 5)、SHA (Secure Hash Algorithm) 等がある。ハッシュ関数の詳細については岡本栄司著「暗号理論入門」(共立出版株式会社)に詳しい。

【0030】最初にデジタルコンテンツからハッシュ対象部分集合と、埋め込み対象部分集合を抽出する。次にハッシュ対象部分集合のデータ値のハッシュ値を求める。ハッシュ対象部分集合のデータ値が変更されると、求めたハッシュ値と一致しなくなる。求めたハッシュ値をデジタルコンテンツと分離することなく保存するために、電子透かしとして埋め込み対象部分集合に埋め込み保存する。

【0031】従って、不正検知の際には、ハッシュ対象部分集合からハッシュ値を求め、埋め込み対象部分集合から電子透かしとして埋め込まれているハッシュ値を抽出し、求めたハッシュ値と抽出したハッシュ値の比較を行い、一致していた場合、正当であると判定する。本発明による不正検知方式では、ハッシュ対象部分集合が改竄された場合、及び埋め込み対象部分集合が電子透かしが正常に抽出できない程度に改竄された場合に不正であると検知する。

【0032】より検知精度を向上させるために、ハッシュ対象部分集合に属するデータ値と埋め込み対象部分集合に属するデータ値とを交互に配置することが考えられる。一例として、デジタルコンテンツとしてデジタル画像を扱うものとし、ハッシュ対象部分集合の画素と埋め込み対象部分集合の画素をデジタルコンテンツ上にラスタ(横のビット列)単位、或いは縦のビット列単位に交互に取る場合や、ビット又はビット列又はデジタルコンテンツ上の矩形等の単位で千鳥状等を取る場合等がある。この際、ハッシュ対象部分集合と埋め込み対象部分集合の和がデジタルコンテンツ全体と一致しているならば、デジタルコンテンツ全体についての改竄が検知される。

【0033】また、部分的な改竄のみを次のようにすることにより検知可能である。即ち、デジタルコンテンツ上のオブジェクト又は部分単位でハッシュ値を求め、求めたハッシュ値を他のオブジェクト或いは部分に埋め込むことにより、オブジェクト単位、部分単位での改竄も検知される。

【0034】次に、不正検知装置202及び電子透かし埋め込み装置をハードウェアで構成した場合の実施の形態について説明する。尚、不正検知装置及び電子透かし埋め込み装置はハードウェア構成の他にソフトウェアに

よるコンピュータシステム構成によっても容易に実現可能である。

【0035】図3は、電子透かし埋め込み装置の第1の実施の形態を示すブロック図である。本装置への入力、デジタルコンテンツ、及び座標値の集合等で表される位置情報である。本装置は記憶装置301、入力された位置情報による制御を受け、デジタルコンテンツよりハッシュ対象部分集合のデータ値を抽出するスイッチ302、2つに分割されたデジタルコンテンツのハッシュ対象部分集合のデータ値よりハッシュ値を計算する演算装置303、計算されたハッシュ値を電子透かしとして、分割されたデジタルコンテンツの第2の部分に埋め込む埋め込み装置304よりなる。ここで位置情報とは、どこに透かしを埋め込むかという座標位置等で表される情報である。

【0036】入力されたデジタルコンテンツのデータ値は、時間的なずれを調節するために一時的に記憶装置301に記憶される。記憶装置301に記憶されたデータ値はスイッチ302に入力され、位置情報により、ハッシュ値を計算されるハッシュ対象部分集合が抽出される。ハッシュ対象部分集合は演算装置303に入力される。演算装置303の計算結果として得られるハッシュ値は、埋め込み装置304に入力され、記憶装置301に保存されていたデジタルコンテンツに電子透かしとして埋め込まれる。

【0037】この際、電子透かしの埋め込みは、位置情報による制御を受け、電子透かしを埋め込む対象は埋め込み対象部分集合内のデータ値となる。また、埋め込み対象部分集合はハッシュ対象部分集合と交わらないため、電子透かしを埋め込むことにより、デジタルコンテンツのハッシュ対象部分集合に含まれるデータ値から計算されるハッシュ値が変化することはない。

【0038】図4は不正検知装置の第1の実施の形態を示すブロック図である。本装置への入力、調査対象のデジタルコンテンツ及び図3の電子透かし埋め込み装置に入力したのと同様の位置情報である。本装置は、時間的なずれを調整する記憶装置401、位置情報による制御を受け入力されたデジタルコンテンツのデータ値から、電子透かしが埋め込まれていないハッシュ対象部分集合を抽出するスイッチ401、図3と同じ方法によりデジタルコンテンツのハッシュ対象部分集合に含まれるデータ値よりハッシュ値を計算する演算装置403、デジタルコンテンツより電子透かしとして埋め込まれているハッシュ値を抽出する電子透かし抽出装置404、ハッシュ対象部分集合より計算したハッシュ値と、デジタルコンテンツより抽出したハッシュ値を比較する比較装置405よりなる。

【0039】本装置に入力された調査対象のデジタルコンテンツは、まず一時的に記憶装置401に記憶される。記憶装置401に保存されたデジタルコンテンツ

は、スイッチ401に入力され、図3と同一の位置情報によりデジタルコンテンツからハッシュ値の演算に用いたハッシュ対象部分集合を抽出する。ハッシュ対象部分集合は演算装置403に入力され、ハッシュ値が計算される。また、記憶装置401に記憶されているデジタルコンテンツは電子透かし抽出装置404に位置情報と共に入力され、デジタルコンテンツに埋め込まれているハッシュ値が抽出される。

【0040】演算装置403により計算されたハッシュ値と、電子透かし抽出装置404によって抽出されたハッシュ値は、比較装置405に輸入されて比較され、一致していたときは、デジタルコンテンツが正当であることを出力し、一致していなかった場合は、デジタル情報コンテンツが不正であることを出力する。

【0041】図5は、電子透かし埋め込み装置の第2の実施の形態を示すブロック図である。本装置は、記憶装置501、入力されたデジタルコンテンツから2値化等の領域検出手段によってハッシュ対象部分集合及び埋め込み対象部分集合を抽出する領域検知装置502、領域検知装置502によって検知されたハッシュ対象部分集合に含まれるデータ値を抽出するスイッチ503、抽出されたデータ値よりハッシュ値を計算する演算装置504、計算されたハッシュ値を電子透かしとして、デジタルコンテンツに埋め込む電子透かし埋め込み装置506よりなる。

【0042】入力されたデータ値は、記憶装置501に記憶される。領域検知装置502は、記憶装置501よりデータ値を読み出し、対象領域を2値化等の方法で検知する。領域検知装置502は、対象領域を決定するための座標情報等を入力される場合もある。記憶装置501に記憶されたデジタルコンテンツはスイッチ503に輸入され、領域検知装置502によって抽出されたハッシュ対象部分集合に含まれるデータ値が抽出される。

【0043】抽出されたデータ値は演算装置504に輸入される。演算装置504の計算結果として得られるハッシュ値は、領域検知装置502の制御を受け、埋め込み装置505に輸入され記憶装置501に保存されていたデジタルコンテンツの埋め込み対象部分集合に電子透かしとして埋め込まれる。

【0044】図6は不正検知装置の第2の実施の形態を示すブロック図である。本装置への入力、調査対象のデジタルコンテンツである。本装置は、記憶装置601、入力されたデジタルコンテンツから2値化等の領域検出手段によってハッシュ対象部分集合及び埋め込み対象部分集合を抽出する領域検知装置602、領域検出装置602によって抽出されたハッシュ対象部分集合に含まれるデータ値を抽出するスイッチ603、抽出されたデータ値よりハッシュ値を計算する演算装置604、デジタルコンテンツの埋め込み対象部分集合より、電子透かしとして埋め込まれているハッシュ値を抽出する

電子透かし抽出装置605、演算装置604により計算されたハッシュ値と、抽出装置605により抽出されたハッシュ値を比較する比較装置606よりなる。

【0045】本装置に輸入された調査対象のデジタルコンテンツは、記憶装置601に記憶される。領域検知装置602は、記憶装置601に記憶されたデジタルコンテンツを入力とし、2値化等の手段により、図5の領域検知装置502と同様のハッシュ対象部分集合、埋め込み対象部分集合を抽出する。領域検知装置602は、対象部分集合を決定するための座標情報等が輸入される場合もある。記憶装置601に記憶されたデジタルコンテンツのデータ値は、スイッチ603に領域検知装置602の出力と共に輸入され、ハッシュ対象部分集合に含まれるデータ値が抽出される。

【0046】抽出されたデータ値は演算装置604に輸入され、ハッシュ値が計算される。また、記憶装置601に記憶されたデジタルコンテンツは、領域検出装置602の制御を受け、電子透かしとして埋め込まれている情報を抽出する抽出装置604に輸入され、埋め込まれているハッシュ値が抽出される。演算装置604により計算されたハッシュ値と、抽出装置605によって抽出されたハッシュ値とが比較装置606で比較され、一致していたときはデジタルコンテンツが正当であることを出力し、一致していなかった場合はデジタルコンテンツが不正であることを出力する。

【0047】図7は、電子透かし埋め込み装置の第3の実施の形態を示すブロック図である。本装置は、記憶装置701、入力されたデジタルコンテンツから2値化等の領域検知手段によってハッシュ対象部分集合及び埋め込み対象部分集合を抽出する領域検知装置702、デジタルコンテンツから領域検知装置702によって検知されたハッシュ対象部分集合に含まれるデータ値を抽出するスイッチ703、抽出されたデータ値よりハッシュ値を計算する演算装置704、計算されたハッシュ値を電子透かしとして、デジタルコンテンツに埋め込む電子透かし埋め込み装置705、領域検出装置702によって検出された領域の位置情報をデジタルコンテンツの所定の位置に埋め込む埋め込み装置706よりなる。

【0048】入力されたデータ値は記憶装置701に記憶される。領域検知装置702は、記憶装置701よりデータ値を読み出し、埋め込み位置情報により示されている所定の位置と重なり合わない領域に存在する、対象領域を2値化等の方法で検知する。領域検知装置702は、対象領域を決定するための座標情報等を入力される場合もある。記憶装置701に記憶されたデジタルコンテンツはスイッチ703に輸入され、領域検知装置702によって抽出されたハッシュ対象部分集合に含まれるデータ値が抽出される。

【0049】抽出されたデータ値は演算装置704に入

力される。演算装置704の計算結果として得られるハッシュ値は、領域検出装置702の制御を受け、埋め込み装置705に入力され記憶装置701に保存されていたデジタルコンテンツの埋め込み対象部分集合に電子透かしとして埋め込まれる。電子透かしの埋め込まれたデジタルコンテンツは埋め込み装置706に入力され、埋め込み対象部分集合、ハッシュ対象部分集合と重なり合わない位置を示す埋め込み位置情報に応じた所定の位置に、埋め込み対象部分集合を特定できる座標値等の位置情報及びハッシュ対象部分集合の同様の位置情報等と共に埋め込まれる。

【0050】図8は不正検知装置のさらに第3の実施の形態を示すブロック図である。本装置への入力は、調査対象のデジタルコンテンツ、及び埋め込み位置情報である。本装置は、記憶装置801、入力されたデジタルコンテンツから、電子透かしとして埋め込まれているハッシュ対象部分集合の位置情報、及び埋め込み対象部分集合の位置情報を抽出する電子透かし抽出装置802、デジタルコンテンツより、領域検出装置802によって抽出されたハッシュ対象部分集合に含まれるデータ値を抽出するスイッチ803、抽出されたデータ値よりハッシュ値を計算する演算装置804、デジタルコンテンツの埋め込み対象部分集合より、電子透かしとして埋め込まれているハッシュ値を抽出する電子透かし抽出装置805、演算装置804により計算されたハッシュ値と、抽出装置805により抽出されたハッシュ値を比較する比較装置806よりなる。

【0051】本装置に入力された調査対象のデジタルコンテンツは、記憶装置801に記憶される。抽出装置802は、記憶装置801に記憶されたデジタルコンテンツを入力とし、所定の位置に電子透かしとして埋め込まれている位置情報より、ハッシュ対象部分集合、埋め込み対象部分集合を特定する。記憶装置801に記憶されたデジタルコンテンツのデータ値は、領域検出装置802の制御を受けるスイッチ803に入力され、ハッシュ対象部分集合に含まれるデータ値が抽出される。

【0052】抽出されたデータ値は演算装置804に入力され、ハッシュ値が計算される。また、記憶装置801に記憶されたデジタルコンテンツが、領域検出装置802の制御を受ける抽出装置804に入力され、電子透かしとして埋め込み対象部分集合に埋め込まれているハッシュ値が抽出される。演算装置804により計算されたハッシュ値と、抽出装置805によって抽出されたハッシュ値は、比較装置806で比較され、一致していたときはデジタルコンテンツが正当であることを出力し、一致していなかった場合はデジタルコンテンツが不正であることを出力する。

【0053】次に本発明の他の実施の形態としての記憶媒体について説明する。本発明はハードウェアで構成することがもきるが、CPUとメモリとで構成されるコン

ピュータシステムで構成することもできる。コンピュータシステムで構成する場合、上記メモリは本発明による記憶媒体を構成する。即ち、前述した実施の形態で説明した動作を実行するためのソフトウェアのプログラムコードを記憶した記憶媒体をシステムや装置で用い、そのシステムや装置のCPUが上記記憶媒体に格納されたプログラムコードを読み出し、実行することにより、本発明の目的を達成することができる。

【0054】また、この記憶媒体としては、ROM、RAM等の半導体メモリ、光ディスク、光磁気ディスク、磁気媒体等を用いてよく、これらをCD-ROM、フロッピーディスク、磁気媒体、磁気カード、不揮発性メモリカード等に構成して用いてよい。

【0055】従って、この記憶媒体を図2～図8に示したシステムや装置以外の他のシステムや装置で用い、そのシステムあるいはコンピュータがこの記憶媒体に格納されたプログラムコードを読み出し、実行することによっても、上記実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【0056】また、コンピュータ上で稼働しているOS等が処理の一部又は全部を行う場合、あるいは記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された拡張機能ボードやコンピュータに接続された拡張機能ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づいて、上記拡張機能ボードや拡張機能ユニットに備わるCPU等が処理の一部又は全部を行う場合にも、上記実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【0057】

【発明の効果】以上説明したように、本発明によれば、電子透かしにデジタルコンテンツの部分集合から演算されたハッシュ値等の値を埋め込むことにより、電子透かしに対してノイズを加えたり、故意に改竄あるいは画像変換等の攻撃等の不正がなされたことを検知することができると共に、不正が検知された場合に、デジタルコンテンツを使用に適さない状態にする等の著作権保護が可能となった。

【図面の簡単な説明】

【図1】本発明を適用できる一般的な公衆ネットワークと公衆ネットワークにつながる機器からなるシステムの構成図である。

【図2】本発明の著作権保護方式のシステムへの搭載例を示す構成図である。

【図3】本発明による電子透かし埋め込み装置の第1の実施の形態を示すブロック図である。

【図4】本発明による不正検知装置の第1の実施の形態を示すブロック図である。

【図5】本発明による電子透かし埋め込み装置の第2の



実施の形態を示すブロック図である。

【図6】本発明による不正検知装置の第2の実施の形態を示すブロック図である。

【図7】本発明による電子透かし埋め込み装置の第3の実施の形態を示すブロック図である。

【図8】本発明による不正検知装置の第3の実施の形態を示すブロック図である。

【符号の説明】

202 不正検知装置

203 演算処理装置

205 コントローラ

\* 301、501、701 記憶装置

302、503、703 スイッチ

303、504、704 演算装置

304、505、705、706 埋め込み装置

502、702 領域検出装置

401、601、801 記憶装置

402、603、803 スイッチ

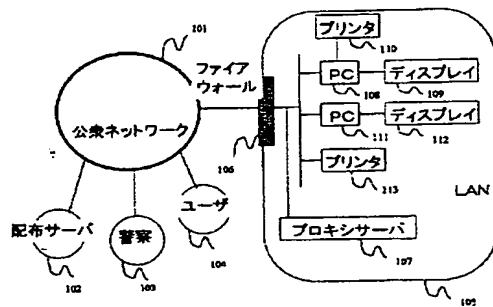
403、604、804 演算装置

404、605、802、805 抽出装置

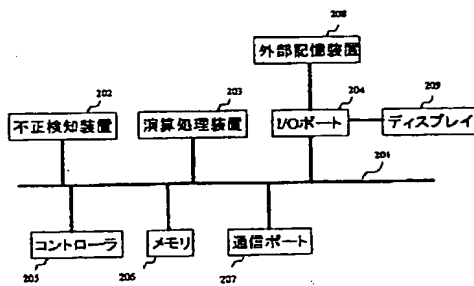
10 405、606、806 比較装置

\* 602 領域検知装置

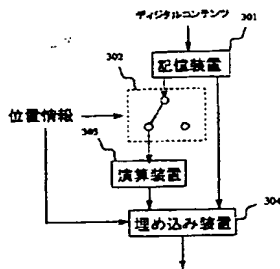
【図1】



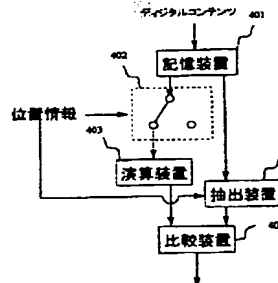
【図2】



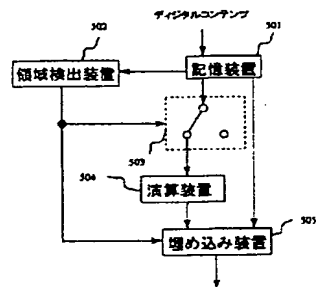
【図3】



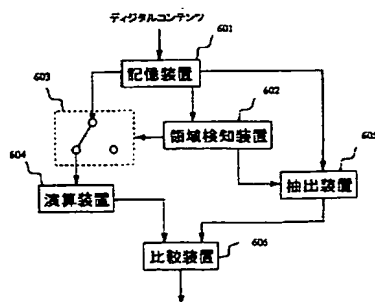
【図4】



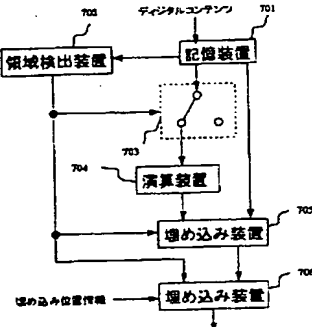
【図5】



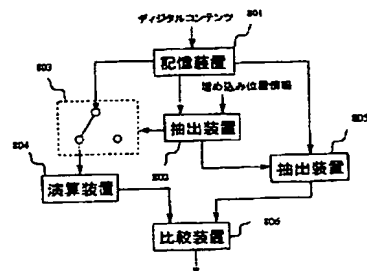
【図6】



【図7】



【図8】



フロントページの続き

(51)Int.Cl.<sup>7</sup>

識別記号

F I

タームコード(参考)

H 0 4 L 12/58

H 0 4 L 11/20

1 0 1 Z

H 0 4 N 1/387

F ターム(参考) 5B057 CE08 CG07

5C076 AA12

5J104 AA08 AA14 LA05 NA12 PA14

5K030 GA15 HB02 HC01 HD01 LA01

5K033 AA08 BA13 DB14 DB18 DB21

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**